Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

The Role of Transnational Cooperation in Cybersecurity Law Enforcement

Adonis Palustre
University of Nevada, Reno
apalustre@unr.edu

David Croasdell
University of Nevada, Reno
davec@unr.edu

Abstract

Cybersecurity has become a significant focal point for law enforcement, businesses, and consumers with the significant advancements made in cyber technologies, cyber use, and cybercrimes, [16]. Organized cybercrime includes activities such as skimming, botnets, provision of child pornography and advance fee fraud. Unorganized cybercrime could be simple fraud, downloading child pornography, trolling or uttering threats. Both organized and unorganized activities have grown more prevalent in today's digital landscape. The media sensationalize breaches, such as the hacking of HBO's Game of Thrones episodes and the Equifax data breach. These incidents get much fanfare shifting focus to law enforcement agencies their plans to address the crimes. We need to know more about the effectiveness of measures against cybercrime and the cooperation between nations against cybercrime. This manuscript examines this issue by exploring how transnational cooperation succeeded in the apprehension of wanted individuals in Operation Avalanche.

1. Introduction

World economies have become more global over the past two decades. Globalization has been mirrored by growth in illicit digital activity. The global impact of transnational crime has risen to unprecedented levels. Criminal groups have diversified their activities, appropriated new technologies and adapted horizontal network structures that are difficult to trace and stop. The result has been an unparalleled scale of international crime. For many reasons, global transnational crime presents nations with a particularly challenging task. By definition, transnational crime crosses borders. But, traditional law enforcement institutions were primarily constructed to maintain order within national boundaries. In addition, transnational crime affects nations in diverse ways. In many states, political institutions have strong links to transnational crime. Citizens in numerous communities across the world rely on international criminal groups to provide basic services. Finally, the international community requires solid data to gauge the challenge and effectiveness of responses. However, data on transnational organized crime is often politicized and notoriously difficult to gather [5].

For almost seven years, Avalanche grew into one of the world's most sophisticated criminal syndicates resembling an international conglomerate staffed by corporate executives, advertising salespeople, and customer service representatives. The business provided a one-stop shop for criminals lacking technical expertise but possessing the motivation and ingenuity to perpetrate a scam. At the peak of their cyber activities, Avalanche helped enable the hijacking of hundreds of thousands of computer systems in homes and businesses around the world [4]. When it comes to the cybercriminal enterprise, a need for a strong and reliable technology is required. What separates large operations, such as Avalanche, from the smaller groups is business acumen [4]. Large enterprises run underground markets, forums and message systems that are often hosted on the deep web. They operate like a 'regular' business buying products to handle their email, spreadsheets and document sharing, and hosting websites on Amazon with payments handled by PayPal [4]. Legitimate service platforms coupled with nefarious means to conduct business have created a service-based economy of cybercrime. In December 2016, everything came to a screeching halt for Avalanche. Europol, the European Union's law enforcement agency, arrested five people and seized 39 computer servers following a four- year-long international investigation of Avalanche. Police agencies representing 30 countries participated in the effort to shut down the group that had caused hundreds of millions of dollars in damage through its cyberattacks [25].

The rapid development of computer connectivity and the role of the internet in the emergence of new e-commerce have compelled national governments and international agencies to address the need for

URI: https://hdl.handle.net/10125/59996
ISBN: 978-0-9981331-2-6

regulation and safety on the information superhighways [2]. Cybercrimes happen on a regular basis and it is very likely that a much bigger and more technically sophisticated cybercrime enterprise will rise up after the demise of Avalanche. It is almost a given that such operations will transcend national borders and will be operated internationally. So, how can law enforcement agencies successfully pursue cyber criminals? The complex transnational nature of cyber investigations requires international cooperation between public and private organizations through information sharing and new cyber legislations at an unprecedented level to successfully impact on top-level cybercriminals.

2. Literature Review: Frameworks for Cooperation

In 1992, the United Nations Economic and Social Council observed that international experience shows that organized crime has crossed national borders to become transnational. Aspects of societal evolution may make powerful criminal organizations even more impenetrable and facilitate the expansion of their illegal activities [23]. A traditional transnational crime would involve terrorism, national privacy, drug trafficking, trafficking in persons, trafficking in arms and other forms of organized crime, all of which threaten national security and undermine sustainable development and the rule of law. The United Nations system assists Member States in their fight against transnational organized crime. A number of international conventions on drug control, and the UN Convention against Transnational Organized Crime and its protocols on human trafficking, migrant smuggling and trafficking of firearms, as well as the 'UN Convention against Corruption', constitute the key framework for a strategic response. The 'United Nations Office on Drugs and Crime' is the guardian of the related international conventions.

Cybercrime creates an unprecedented need for concerted action from government and industry, but also unprecedented challenges to effective international cooperation. An offense may produce victims in many countries, as in cases involving virus attacks, copyright violations, and other offences carried out globally through the internet. This in turn may result in cross-border conflicts regarding which jurisdiction(s) should prosecute the offender and how such prosecutions are carried out to avoid inconvenience to witnesses, duplication of effort, and unnecessary competition among law enforcement officials [3].

Keeping this in mind, regional international organizations were formed in an effort to maintain cybersecurity and harmonize international measures to combat cybercrime. Some these organizations are listed below along with their strategies to combat cybercrime.

In 1990, the United Nations (UN) General Assembly adopted a resolution on computer crime [23]. In 2000, the same body adopted a resolution to combat the criminal misuse of information technology. In 2002; it adopted a second resolution on the criminal misuse of information technology [6]. The G8, comprised of the heads of eight industrialized countries: the United States, the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada, supported the position through a public announcement. The communiqué mandated that all law enforcement personnel be trained and equipped to address cybercrime. In included an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. Further, the resolution stipulated that member countries have a point of contact on a 24 hour a day, 7 days a week basis [29].

In 2001, the 47 member-state Council of Europe (CoE) established the first international Convention on Cybercrime in association with 25 other countries across the globe. The Convention addresses crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer- related fraud, child pornography and violations of network security [1]. The Convention, apart from enhancing mutual legal assistance (MLA), provides comprehensive powers to:

- expedite reservation of stored computer data and partial disclosure of traffic data
- make production orders
- search computer systems; to seize stored computer data
- enable real-time collection of traffic data; and to intercept the content of questionable electronic data [2].

The main objective of the European Convention is to adopt a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

Various regional frameworks were established in the early 2000s to address the growing need to pursue transnational cybercrimes. The Asia-Pacific Economic Cooperation (APEC) issued a mandate in August 2002 to combat cybercrimes at the regional level and provide assistance to international conventions. Their cyber security strategy is intended to assist economies in the region to enhance their legislative frameworks to combat cybercrime and to

promote the development of law enforcement investigative capacity to effectively deal with cybercrime [2]. The Organization for Economic Co-operation and Development (OECD) is comprised of 34 countries. In 2002, the organization published "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" [1]. In 2002, the Commonwealth of Nations presented a model law drafted in accordance with the Convention on Cybercrime, which provides a legal framework that harmonizes legislation within the Commonwealth and enables international cooperation [1]. The Economic Community of West African States (ECOWAS) is a regional group of western African countries founded in 1975 and it has fifteen-member states. In 2009, ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law [10]. The foundation for new and international rules is now in place. Over the last two years, there has been important progress in developing global cybersecurity norms. For example, in July 2015 governmental experts from 20 nations recommended cybersecurity norms for nation-states "aimed at promoting an open, secure, stable, accessible and peaceful ICT environment" [24]. These include key principles that bar governments from engaging in malicious activity using information and communications technology or similarly damaging other nations' critical infrastructure. Importantly, leading governments have also proven that they can address these issues through direct and frank bilateral discussions. The U.S. and China agreed to important commitments pledging that neither country's government would conduct or support cyber-enabled theft of intellectual property in 2015 [26]. This paved the way for the Group of 20 to affirm the same principle more broadly at its meeting just two months later [9] and additional inter-governmental discussions are continuing to progress further today.

3. Case Study: Operation Avalanche

Since 2009, the Avalanche network was used as "delivery platform to launch and manage mass global malware attacks and money mule recruiting campaigns" [7]. The Avalanche infrastructure was setup to conduct malware, phishing, and spam activities. They also sent one million emails with damaging attachments or links every week to unsuspecting victims. On any given day, 500,000 computers around the world were infected by the Avalanche network [8]. Members of the Avalanche group were able to gain access to bank records and email passwords of victims after infecting their computers with malware. Once the money was stolen, the cybercriminals used several highly organized networks of mules to purchase goods, which enabled them to launder the illicitly obtained money. The group targeted more than 40 major financial institutions [17]. Avalanche caused an estimated 6 million euros in damages on online banking systems in Germany alone [7]. The United States' Department of Justice estimates that the damage worldwide caused by these cyber-attacks to be hundreds of millions of dollars. The exact amount is difficult to calculate due to the high number of malware families present on the network [25].

Avalanche was attractive to cybercriminals because it used a so-called fast-flux network (see Appendix 1) to defend itself from disruption and identification. Fast- flux is an evasion technique used by botnet operators to quickly move a fully qualified domain name from one or more computers connected to the internet to a different set of computers. The double fast-flux technique used by Avalanche changes both the IP address records and a component called a name server that is used to match the IP addresses and domain. This makes it difficult to understand a computer network and to disrupt it [21]. Malware campaigns distributed by this network include goznym marcher, matsnu, nymaim, urlzone, virut, xswkit, pandabanker, rovnix, teslacrypt, kbot, ranbyus, vm zeus, kins, CoreBot, Dofoil, GOZI2, Slempo, Trusteer App and Vawtrack.

Investigations started in 2012 in Germany after encryption ransomware (the so-called Windows Encryption Trojan) infected a substantial number of computer systems, blocking users' access. It is estimated that millions of private and business computer systems were infected with malware, enabling the cybercriminals operating the network to harvest bank and email passwords [7]. After four years of investigation, the Avalanche network was taken down. In December 2016, the Public Prosecutor's Office of Verden and the Luneburg Police (Germany) in close cooperation with the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice, and the Federal Bureau of Investigation, the Europol, Eurojust, and global partners from all over 40 countries dismantled the international criminal infrastructure platform of Avalanche [7, 25]. The global effort to take down Avalanche resulted into the arrest of five individuals, search of 37 premises, and seizure of 39 servers. It resulted into 221 Avalanche servers taken offline.

Sink holing is a technique whereby "traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security

company" [7]. When employed to its full capacity, infected computers can no longer reach the criminal command and control computer systems; Criminals can no longer control the infected computers. The Avalanche sting operation is considered to be the largest ever use of sink holing to combat botnet infrastructures. It is unprecedented in scale with over 800,000 domains seized, sink holed or blocked [7].

3.1 The Uberisation of International Police Work

Rob Wainwright, director of Europol, provided an interesting insight about the future of international cooperation when it comes to combatting cybercrime in the future [29]. Wainwright believes that platform economy industries such as Uber and Airbnb can serve as a business model for the future of international police work. Uber is the largest taxi company in world and yet do not own a single taxi while Airbnb is the world's largest provider of accommodations but do not own a single property. He adds that international police agencies such as the Interpol and Europol can bring about this information exchange between local law enforcement agencies. During the World Economic Forum 2016 held in Davos-Klosters, Switzerland, he released this statement:

> *"At Davos I have been making the case for following the same approach on security. For the last six years it's the business concept we have developed at Europol. Our Uber-like theme is that Europol has become one of the leading law enforcement agencies in the world but has no police powers and no unique intelligence of its own. Instead its innovative technology-enabled platform connects over 500 law enforcement agencies from Europe and beyond and carries a level of information exchange between those partners that has quadrupled in less than five years. The platform works through its ability to connect and collect across a large community and, crucially, by applying the power of data analytics at the hub of this information eco-system in Europol's HQ. As more and more partners are attracted to this community the continued growth of the model seems certain, as are further improvements in the output of this system: operational services that help national authorities fight crime and terrorism."* [27]

Based on this recommendation, the future of international police work lies on information sharing between local, national, regional, and international police agencies and private corporations. The world simply cannot rely on just the state actors and local law enforcement to deal with cybercrimes because "over-reliance on the state, especially the public police, to address cyber-security issues would expose both markets and society to frequent low level but costly risks" [19]. Regional police networks that facilitate transnational cooperation such as the Europol, Police Community of the Americas (Ameripol), Association of Southeast Asian Nation's Association of National Police Agencies (ASEANAPOL), and Interpol can play a huge role as the information sharing platform for their regions as well as the rest of the world. In order to realize this, a regional framework must be established that allows for information sharing from local police agencies to the national and then regional levels. To ensure the success of this information sharing, nations will have to create new legislations that will facilitate such cooperation between regional police groups and transnational cooperation between countries. Platforms of cooperation already exist and can serve as a model for future legislative and law enforcement examples. The Interpol already has a new digital center in Singapore and is used as a base of operation for cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support, and partnerships [12].

Information sharing should not be limited between governments and law enforcement agencies. The involvement of private parties such as telecommunications corporations, software companies, and non-government organizations are also important. These organizations can provide subject-matter expertise when it comes information and communication technologies. More often than not, these organizations are highly proficient in their use of technology and other resources and their knowledge in cyber issues is vast. Companies from various industries ranging from Microsoft, IBM, McAfee, AT&T, Sony, and Wells Fargo have a vested interest in assisting law enforcement agencies in the successful arrest of cybercriminals. Since it is their products and services that are affected by cyber-attacks, companies benefit from the cooperation and information sharing in order to pursue the wrongdoers. The Shadowserver Foundation, a non-profit organization who continually seeks to "provide timely and relevant information to the security community at large" [18], played an important role in the take down of Avalanche. As a key member of the technical subgroup in Operation Avalanche, the Shadowserver Foundation worked with partners to build the sink holing infrastructure and coordinate the international DNS Registry activities. Such level of expertise is found in non-government organizations and private companies and this is why their involvement in information sharing is essential.

Current public-private party partnerships in cybersecurity are already in place all over the world and can serve as a model for other partnerships to emulate [15]. The National Cyber-Forensics and Training Alliance (NCFTA) is an alliance between the Federal Bureau of Investigation, U.S. Postal Inspection Service, and the private industry. The NCFTA also hosts other partnerships such as the Digital PhishNet platform that allows for a public-private cooperation to drive enforcement against phishing websites. The European Financial Coalition connects Europe's law enforcement with the IT and finance industries to fight child exploitation online. At the end of the day, the user affected needs to have a part in the information sharing of potential cyber threats. Signal-Spam, a public-private partnership, allows users to report anything they consider to be spam in their email client in order to assign it to the public authority or the professional that will take the required action to combat the reported spam. This type of partnership between end users and private corporations can serve as a model for future partnerships on bigger cybersecurity issues.

4. Recommendation: Prevention is better than cure

Cybercriminals and threat actors are people too. Since they have to earn a living, they make mistakes just like we do; they are influenced by their environments just like we are. We must consider the social, cultural, and economic factors driving these individuals to commit a crime. In order to prevent or even simply discourage cybercriminals from committing a crime, the developing world must catch up with their developed counterparts in terms of technology advancement, economic opportunities, policy making because many of the cybercrimes happening in this world originated from the developing world [13]. At the extreme of the risks now posed, cybercriminals operating in the context of failed or failing states contribute to the criminalization of the world economy by providing both safe havens and plundered resources [11]. Kellerman argues that the developing world sees no incentive to collaborate with the United States and its allies when it comes to improving their ICT infrastructures. He believes it is "paramount to the success of our efforts that we provide financial incentives to the developing world so that they can both create a more secure local cyberspace and assist in managing the systemic risks associated with the widespread compromise of their networks." [13]

The development of the ICT infrastructures of the developing world relies heavily on programs created by international aid agencies as well as non-governmental organizations. The World Bank spent billions of dollars connecting the developing world to the internet through its Information and Communications Technology (ICT) projects and other e-finance initiatives. The World Bank can serve as a "stabilizing force in providing grants that harden financial and telecommunications and infrastructures overseas and in encouraging other countries to cooperate and help manage the systemic cyber risk posed by the current widespread infestation of these global infrastructures [13]. Current World Bank programs on strengthening the ICT infrastructures of the developing world is important but one international actor is not enough to enable the developing world to catch up with their developed counterparts. The United Nations is a strong advocate of strengthening the ICT infrastructures of the world and they believe that it is one of the key drivers behind the implementation of all the Sustainable Development Goals [28]. The Whitaker Peace and Development Initiative envisions connectivity that can help vulnerable communities on their path to peace and resilience [28] and this non- governmental organization has invested on the ICT infrastructures of South Sudan and Uganda.

Investments on the critical ICT infrastructures of the developing part of the world is not the only thing that we need to do to prevent cybercrimes from happening in the future. We must also discourage the technologically savvy individuals from embracing the criminal world and push skilled labor towards the whitehat community [13]. The International Multilateral Partnership Against Cyber Threats (IMPACT) is the leading non-governmental organization in this aspect. Based in Malaysia and partnered with the United Nations and the International Telecommunications Union, IMPACT is a neutral body that disseminates and promotes best practices in information security to a large portion of the world. This organization drives training and capacity building in developing nations in a politically neutral fashion -- which will inevitably increase trust between nations [13].

5. Discussion

The establishment of regional and international cooperation present challenges. Le Toquin [15] identified three:

- Jurisdictional variations on data retention and sharing of evidence
- Lack of communication between law enforcement and service providers regarding sharing and obtaining needed evidence most

efficiently
- Tension between privacy and needs of data retention for enforcement purposes

Challenges like these argue for regionally agreed upon and ratified resolutions. It is important to establish up a framework for transnational law enforcement and cooperation among affected parties. Assemblies to form this kind of cooperation must clearly state and define the terms of information sharing--what should be shared and who can access it and when can it be accessed. A possible challenge that could present itself is the infringement of a nation's sovereignty when it comes to sharing information. For other countries, a regional framework may not work and they may not see it fit on how their law enforcement agencies operate. But cooperation is still needed due to the borderless nature of cybercrimes. Bilateral or even multilateral agreements between nations involved are an option without being part of a binding regional agreement. This way, the availability of information can be shared only to the parties involved without putting it in an information database that is readily available for anyone.

Organized cybercriminal organizations like Avalanche will come and go but there is still the looming threat of potential nation-state cyber-attacks. Cyberspace is considered the fifth arena of warfare after land, sea, air, and space. Just like the ideas discussed before in this paper, threats of a nation-state cyber-attack can still be resolved in the same manner as a regular cybercrime: through transnational cooperation between law enforcement agencies, private sectors, and non- government organizations. The RSA Conference in San Francisco held in 2018 brought the world's security professionals together to discuss cybersecurity with an emphasis on this issue. The past year has witnessed not just the growth of cybercrime, but a proliferation in cyber-attacks that is both new and disconcerting. This has included not only cyber-attacks mounted for financial gain, but new nation-state attacks as well [20]. In his Microsoft blog, Brad Smith, President and Chief Legal Officer at Microsoft, wrote the following:

> "*Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."* [20]

The Geneva Convention, in simple terms, is the rules of engagement when it comes to war. The protection of civilians, provisions against torturing a prisoner-of-war, the unnecessary destruction of cultural or religious buildings, the protection of women and children in times of war, and the recognition of the neutrality of medics are all mentioned in the Geneva Convention. Smith's calling for a Digital Geneva Convention highlights the "rules" of engaging cyber-attacks:

1. No targeting of tech companies, private sector, or critical infrastructure
2. Assist private sector efforts to detect, contain, respond to, and recover from events
3. Report vulnerabilities to vendors rather than stockpile, sell, or exploit them
4. Exercise the restraint of developing cyber-weapons and ensure that any developed are limited, precise, and not reusable
5. Commit to nonproliferation activities to cyber-weapons
6. Limit offensive operation to avoid a mass event

In his blog, Smith added the creation of the Digital Switzerland, a neutral body trusted by everyone to adhere to these rules as well as be the guiding force when it comes to cyber-attacks and cybercrimes. Smith believes that Microsoft can be this Digital Switzerland since they are one of the world's leaders in information technology and they have the resources to be successful at it. Smith also believes that he works for the "United Nations of Information Technology" by being in Microsoft [20].

All these points that Smith mentioned in his blog further reinforces the idea that the private sector plays a huge role in the successful pursuit of any cyber-based crimes or attacks. Transnational law enforcement cooperation is good but the involvement of private ICT companies will make such a cooperation more effective. Technical resources are readily available for many of these private companies and they are the first line of defense of protecting the civilians and consumers when it comes to these attacks. A mutually agreed upon digital Geneva Convention will also allow nations to develop their own legal framework to pursue and prosecute cybercriminals as well as establish cooperation protocols with other nations.

6. Conclusions

Better frameworks and partnerships will be needed as soon as new and more technologically savvy cyberthreats emerge. The nations of this world will need to adapt in the ever-changing nature of cybercrimes. The solution to the transnational nature of cybercrimes lies in the partnership between states and private corporations to form alliances to pursue the criminals through information sharing with the help of a regional and/or international policing networks such as Europol. The need to address root causes of these crimes is crucial. The developing world needs to catch up with the rest of their developed counterparts in technology as well as legislation developed nations must help international aid agencies such as the World Bank to realize this goal.

7.0 References

[1] Ajayi, E. F. G. (2006) "Challenges to enforcement of cyber-crimes laws and policy", Journal of Internet and Information Systems, Vol. 6 Issue: 1, pp. 1-12.

[2] Broadhurst, R. (2006) "Developments in the global law enforcement of cyber-crime", Policing: An International Journal of Police Strategies and Management, Vol. 29 Issue: 3, pp. 408-433.

[3] Bullwinkel, J. (2005), "International cooperation in combating cybercrime in Asia: existing mechanisms and new approaches", Cyber-crime: The Challenge in Asia, University of Hong Kong Press, Hong Kong.

[4] Cillufo, F., Nadeau, A., & Wainwright, R. (2017) "Police around the world learn to fight global-scale cybercrime", PhysOrg. Retrieved November 13, 2017, from https://phys.org/news/2017-04-police-world-global-scale-cybercrime.html

[5] Council on Foreign Relations (2013) "The Global Regime for Transnational Crime", Retrieved November 14, 2017, from https://www.cfr.org/report/global-regime-transnational-crime

[6] Cowdery, N. (2008). "Emerging Trends in CyberCrime, 13th Annual Conference - New Technologies in Crime and Prosecution: Challenges and Opportunities", International Association of Prosecutors.

[7] Europol. (2016) "Avalanche Network Dismantled in International Cyber Operation", Europol Press Release. Retrieved November 14, 2017 from https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

[8] Fatzick, J. (2016) "Europol Brings Down Global Crime Syndicate", VOA News. Retrieved November 14, 2017 from https://www.voanews.com/a/europol-brings-down-avalanche-global-cybercrime-syndicate/3619096.html

[9] G20. (2015) "G20 Leaders' Communique agreed in Antalya" Retrieved December 3, 2017, from http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/

[10] Gercke, M. (2010) "Regional and international Trends in Information Security Issues", Cybercrime Research Institute.

[11] Gros, J. (2003) "Trouble in paradise: crime and collapsed states in the age of globalization", British Journal of Criminology, Vol. 43, pp. 63-80.

[12] Interpol. (2017) "About the Interpol Global Complex for Innovation". Retrieved November 14, 2017 from https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for- Innovation

[13] Kellerman, T. (2010) "Building a foundation for global cybercrime law enforcement", Computer Fraud and Security, Vol 2010, Issue: 5, pp. 5-8. Retrieved November, 14 2017 from http://www.sciencedirect.com/science/article/pii/S1361372310700518

[14] Jazri, L. C. (2011) "Cyber Crime and Traditional Crime -Are they connected?", e-Security -Cyber Security Malaysia.

[15] Le Toquin, J. (2006) "Public-Private Partnerships against cybercrime", a presentation to the Organization for Economic Cooperation and Development (OECD). Retrieved November 14, 2017 from http://www.oecd.org/sti/consumer/42534994.pdf

[16] Orton, E. (2014) "Creating a Model of Cyber Proficiency: Remodeling Law Enforcement Tactics in Pittsburgh to Address the Evolving Nature of Cybersecurity", Pittsburgh Journal of Technology Law and Policy, Vol. 14 Issue: 2, pp. 276-279.

[17] Rosenquist , M. (2016) "Avalanche Cybercriminal Infrastructure Takedown", Intel Article. Retrieved November 14, 2017 from https://software.intel.com/en- us/blogs/2016/12/16/avalanche-cybercriminal- infrastructure-takedown

[18] Shadowserver Foundation (2017) "Mission Statement and Introduction". Retrieved November 14, 2017 from https://www.shadowserver.org/wiki/pmwiki.php/Shado wserver/Mission

[19] Shannon, J. and Thomas, N. (2005) "Human security and cyber-security: operationalising a policy framework", in Broadhurst, R. and Grabosky, P. (Eds),

Cyber-crime: The Challenge in Asia, University of Hong Kong Press, Hong Kong.

[20] Smith, B. (2017) "The Need for a Digital Geneva Convention." Retrieved December 3, 2017, from https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ #_ftn1

[21] U.K. National Crime Agency. (2016) "UK helps dismantle Avalanche global cyber network sending 1m fraudulent emails a week". Retrieved November 14, 2017, from http://www.nationalcrimeagency.gov.uk/ news/962-avalanche-takedown

[22] United Nations. (n.d.) "Rule of Law: Transnational Organized Crime", Retrieved November 30, 2017, from https://www.un.org/ruleoflaw/thematic-areas/transnational-threats/transnational- organized-crime/

[23] United Nations Commission on Crime Prevention and Criminal Justice (2001) "Conclusions of the study on effective measures to prevent and control high-technology and computer-related crime", 10th Session, 8–17 May, http://www.unodc.org/pdf/crime/10_ commission/4e.pdf

[24] United Nations General Assembly (2015) "Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security." 70th Session, Item 93. Retrieved December 3, 2017, from http://www.un.org/ ga/search/view_doc.asp?symbol=A/70/174

[25] U.S. Department of Justice. (2016) "Joint Statement on Dismantling of International Cyber Criminal Infrastructure Known as Avalanche". Retrieved November 14, 2017, from https://www.justice.gov /opa/pr/joint-statement-dismantling-international-cyber- criminal-infrastructure-known-avalanche

[26] U.S. Office of the Press Secretary (2015) "Fact Sheet: President Xi Jinping's Visit to the United States." Retrieved December 3, 2017, from https://obamawhitehouse.archives.gov/ the-press-office/ 2015/09/25/fact-sheet-president-xi-jinpings-state-visit- united-states

[27] Wainwright, R. (2016) "The 'Uberisation' of international police work", LinkedIn Article as written by Rob Wainwright. Retrieved November 14, 2017 from https://www.linkedin.com/pulse/uberisation-international-police-work-rob-wainwright

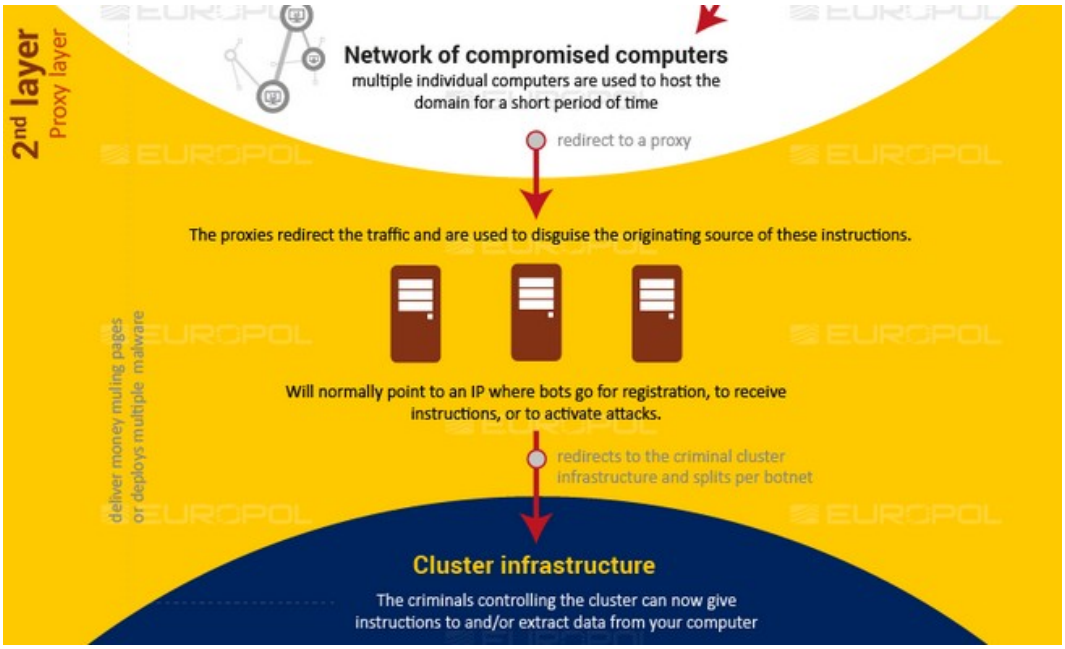
[28] Whitaker, F. (2017) "Sustainable Development Goal 9: Investing in ICT access and quality education to promote lasting peace", General Assembly Speech. Retrieved November 14, 2017 from http://www.un.org/sustainabledevelopment/blog/2017 /0 6/sustainable -development-goal-9-investing-in-ict-access-and-quality-education-to-promote-lasting-peace/

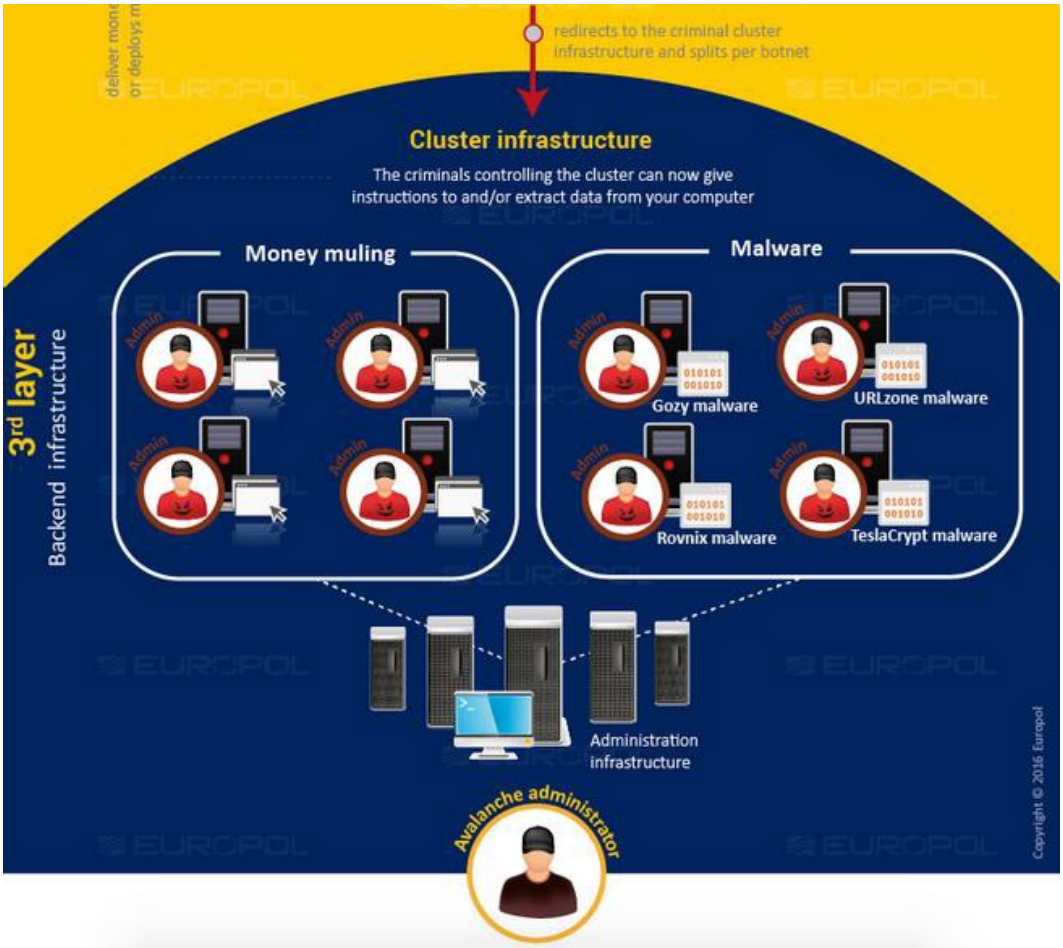
[29] Xingan, L. (2007). "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene". Weboloy. Retrieved November 30, 2017 from http://www.webology.org/ 2007/v4n3/a45.html

8.0 Appendix

Appendix 1: Operation Avalanche's infrastructure

A high resolution infographic is vailable at:
h ttps://www.europol.europa.eu/sites/default/files/images/editor/avalanche_-_double_flux-_simple.png


2nd layer
Proxy layer
Network of compromised computers
multiple individual computers are used to host the domain for a short period of time
redirect to a proxy
The proxies redirect the traffic and are used to disguise the originating source of these instructions.
deliver money muling pages or deploys multiple malware
Will normally point to an IP where bots go for registration, to receive instructions, or to activate attacks.
redirects to the criminal cluster infrastructure and splits per botnet
Cluster infrastructure
The criminals controlling the cluster can now give instructions to and/or extract data from your computer


redirects to the criminal cluster infrastructure and splits per botnet
Cluster infrastructure
The criminals controlling the cluster can now give instructions to and/or extract data from your computer
3rd layer
Backend infrastructure
Money muling
Malware
Gozy malware
URLzone malware
Rovnix malware
TeslaCrypt malware
Administration infrastructure
Avalanche administrator
Copyright © 2016 Europol